EXHIBIT A

Workspace Administrator,

You are receiving this email because a federal court recently ordered that notice be sent to all Enterprise Dasher account holders (i.e., End Users) who may be class members in a class action filed against Google in July 2020 titled, *Rodriguez et al., v. Google LLC* pending in the United States District Court for the Northern District of California, Case No. 3:20-cv-04688-RS.

We are still finalizing the details of when notice will be distributed to End Users but, for now, we know that they will be sent to your End Users by email and wanted to keep you apprised and ask that you consider and satisfy any obligations that you may have under the Google Workspace Terms of Service, including those outlined in Sections 3 and 7 as a result of this notice. We are sending this notice consistent with our obligations under these Terms. More detail about the case, email notices, and proposed next steps are provided for you below.

Case overview

- Four Google account holders ("Plaintiffs") filed a class action lawsuit against Google LLC ("Google") alleging that Google unlawfully accessed their devices and data, even though Web & App Activity ("WAA") and/or supplemental Web & App Activity ("sWAA") were turned off or "paused."
- Plaintiffs allege Google unlawfully accessed their mobile devices to collect, save, and use data concerning their activity on non-Google apps that have incorporated certain Google software code into the apps while WAA and/or sWAA were turned off or "paused."
- Plaintiffs assert three legal claims against Google: 1) invasion of privacy; 2) intrusion upon seclusion (similar to invasion of privacy); and 3) violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA"). For all three legal claims Plaintiffs seek money damages and changes to Google's practices.

Google denies Plaintiffs' legal claims and does not admit to any wrongdoing. The Court has not decided who is right.

Who is in the class?

- The Court certified four classes to assert claims for damages, defined as:

  Comprehensive Computer Data Access and Fraud Act ("CDAFA")

  For the alleged violation of the CDAFA, the Court certified the following classes:

  Class 1: All individuals who, during the period beginning July 1, 2016 and continuing through [NOTICE DATE TK], (a) had their "Web & App Activity" and/or "supplemental Web & App Activity" setting turned off and (b) whose activity on a non-Google-branded

mobile app was still transmitted to Google, from (c) a mobile device running the Android operating system, because of the Firebase Software Development Kit ("SDK") and/or Google Mobile Ads SDK.

Class 2: All individuals who, during the period beginning July 1, 2016 and continuing through [NOTICE DATE TK], (a) had their "Web & App Activity" and/or "supplemental Web & App Activity" setting turned off and (b) whose activity on a non-Google-branded mobile app was still transmitted to Google, from (c) a mobile device running a non-Android operating system, because of the Firebase SDK and/or Google Mobile Ads SDK.

Invasion of Privacy and Intrusion Upon Seclusion

For the alleged invasion of privacy and intrusion upon seclusion legal claims, the Court certified the same Class 1 and Class 2 but excluded individuals who only have an "Enterprise" account or "supervised Google Account for users under age 13" (also known as a "Unicorn" account). An "Enterprise" account is an account managed by an administrator that is designed for use by end users within an organization, such as businesses, non-profits, and schools. A "supervised Google Account for users under age 13" is an account created for a minor when they are under the age of 13, which is created and supervised by a parent using Google Family Link.

Class 1: All "non-Enterprise" and "non-Unicorn" individuals who, during the period beginning July 1, 2016 and continuing [NOTICE DATE TK], (a) had their "Web & App Activity" and/or "supplemental Web & App Activity" setting turned off and (b) whose activity on a non-Google-branded mobile app was still transmitted to Google, from (c) a mobile device running the Android operating system, because of the Firebase Software Development Kit ("SDK") and/or Google Mobile Ads SDK.

Class 2: All "non-Enterprise" and "non-Unicorn" individuals who, during the period beginning July 1, 2016 and continuing through [NOTICE DATE TK], (a) had their "Web & App Activity" and/or "supplemental Web & App Activity" setting turned off and (b) whose activity on a non-Google-branded mobile app was still transmitted to Google, from (c) a mobile device running a non-Android operating system, because of the Firebase SDK and/or Google Mobile Ads SDK.

- Enterprise and supervised Google Accounts for users under age 13 are not included in the Classes for the legal claims for damages for invasion of privacy and intrusion upon seclusion. Although these accounts may have been eligible to be included in the Classes certified for these legal claims, the Court granted Google's request to exclude Enterprise accounts and supervised Google Accounts for users under age 13 from the invasion of

privacy and intrusion upon seclusion Classes. Enterprise and supervised Google Accounts for users under age 13 are still included in the Classes certified for violations of the CDAFA.

- Enterprise and supervised Google Accounts for users under age 13 are within all Classes that have been certified to seek changes to Google's practices.

Email notices

- The Court has ordered that notice be sent to Enterprise accounts that had their WAA and/or sWAA setting turned off from July 1, 2016 to [NOTICE DATE TK] to inform them of their "change in status"—i.e., that they are no longer members of the class for all claims but may still be eligible for damages recovery for one claim, and injunctive relief for all claims.
- On or around [NOTICE DATE TK], Google will provide the court appointed Class Notice Administrator (Epiq) with the names and email addresses of End Users if Google's records indicate that they may be Class Members. The Class Notice Administrator, will be sending notice by email starting [30 days from when the Court approves the parties' proposed notice plan] to all End User Accounts that had their WAA and/or sWAA setting turned off from July 1, 2016 to [NOTICE DATE TK] regardless of who turned off the setting (either, End User or Administrator) using information provided by Google and designated by Google as Highly Confidential - Attorneys' Eyes Only under the court approved Protective Order in this case.
- Epiq will be allowed to share limited information, including information pertaining to individual Class Members, with Plaintiffs' lawyers ("Class Counsel") but only subject to appropriate steps to maintain the security of that data (such as remote access to Class Counsel without transferring the table). Class Counsel may seek access to this information, for example, in the event they receive inquiries from potential Class Members. The information will remain stored and secured by Epiq, and Class Counsel will not print or transfer copies of the list or portions of it (electronic or otherwise), outside of Epiq.

Next steps

- Please consider and satisfy any obligations that you may have under the Google Workspace Terms of Service in light of this notice—i.e., please prepare to receive and/or distribute notice as you would for any other legal notice and/or update.
- The Email Notice sent to Class Members will provide a contact number and additional resources for you and your End Users to request and receive additional information about whether any of your End Users qualify as Class Members.

Additional information

If you have any questions or need additional information, please visit www.xxxxxxxxxx.com or call toll-free at 1-xxx-xxx-xxxx.